UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/578,177	12/15/2006	Makoto Saito	290398US2PCT	5196

22850 7590 10/15/2010

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
10/15/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/578,177	SAITO ET AL.	
	Examiner	Art Unit	
	ARAVIND K. MOORTHY	2492	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 July 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *26,30-32 and 34-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *44-51* is/are allowed.

6)☒ Claim(s) *26,30-32 and 34-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 May 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on 23 July 2010.

2. Claims 26, 30-32 and 34-51 are pending in the application.

3. Claims 26, 30-32 and 34-43 have been rejected.

4. Claims 44-51 have been allowed.

5. Claims 1-25, 27-29 and 33 have been cancelled.

Response to Arguments

6. Applicant's arguments filed 23 July 2010 have been fully considered but they are not persuasive.

On page 20, the applicant argues, regarding claims 26, 30-32 and 34, that Birger fails to disclose the claimed features for establishing a third encrypted communication channel using the public key between the first apparatus and the second apparatus.

The examiner respectfully disagrees. Birger discloses that in ICL session activity, the holder of an identity establishes a communication channel to another identity and exchanges data using the communication channel. The authentication service, using information in the authentication database, provides bi-directional authentication to both parties. The presence and availability management database is consulted to translate the remote identity into its corresponding underlying network address. The identity database may be consulted to look up and translate identity names. Policies from the policy database control the authorization of whether the session is permitted and the parameters that determine the level of security to be employed during data exchange.

On pages 20 and 21, the applicant argues, regarding claims 35, 36, 40 and 42, that Birger fails to disclose the claimed features of “storing a name of the first apparatus and identification information of the first encrypted communications channel in a storage device", "receiving a message including a name of the first apparatus via the first encrypted communication channel" and "determining whether the name included in the message is correct by comparing the name included in the message with the name that is stored in the storage device and that is associated with the identification information of the first communication channel".

The examiner respectfully disagrees. Birger discloses a unique identifier for the device. The examiner asserts that the unique identifier is the name of the first apparatus. The unique identifier is used for authenticating the device.

On page 21, the applicant argues, regarding claims 37-39, 41 and 43, that Birger fails to disclose the claimed features of “receiving, from the first apparatus via the first encrypted communication channel, a message including a first header indicating reliability of a route between the first apparatus and the session management apparatus" and "adding a second header indicating reliability of a route between the session management apparatus and the second apparatus to the message, and sending the message to the second apparatus”.

The examiner respectfully disagrees. Birger discloses an implementation of the ICL software 612 may have available several alternative implementations of the local address layer 616, with each implementation corresponding to a particular choice of network and protocol. The global address layer 615 selects from among these alternative implementations to determine a particular network and a particular protocol to use. The local address layer 616 carries out the selected protocol, including encapsulating application data in network messages as dictated by

the selected protocol, and interacting with the initiating networking software 613. For example, a local address layer implementation intended for a simple message framing protocol atop TCP may prepend each message with a message length indication, and send the encapsulated message that includes the message length indication using the native network's implementation of TCP. In another example, a local address layer implementation intended for HTTP may insert the message into the body of a HTTP GET message, with headers and other information included as dictated by the HTTP protocol specification.

Allowable Subject Matter

7. Claims 44-51 are allowed over the prior art.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 26, 30-32 and 34-43 are rejected under 35 U.S.C. 102(e) as being anticipated by Birger et al US 2009/0006850 A1 (hereinafter Birger).

As to claim 26, Birger discloses a method for establishing an encrypted communication channel between a first apparatus and a second apparatus, wherein:

> a public-key management apparatus and the first apparatus exchange key information used for performing encrypted communication (i.e. The exchange of session key information.) [0211], and the public-key management apparatus and

the first apparatus perform mutual authentication so that a first encrypted communication channel is established (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209];

the public-key management apparatus and the second apparatus exchange key information used for encrypted communication, and the public-key management apparatus and the second apparatus perform mutual authentication so that a second encrypted communication channel is established [0219-0222];

the first apparatus generates a secret key and a public-key, and sends the public-key to the public-key management apparatus via the first encrypted communication channel [0219-0222];

the public-key management apparatus stores the received public-key in its storage device, and the second apparatus obtains the public-key from the public-key management apparatus via the second encrypted communication channel so that a third encrypted communication channel using the public-key between the first apparatus and the second apparatus is established [0219-0222].

As to claim 30, Birger discloses a public-key management apparatus for managing public-keys used for establishing an encrypted communication channel between a first apparatus and a second apparatus, the public-key management apparatus comprising:

a part for exchanging key information for encrypted communication with the first apparatus (i.e. The exchange of session key information.) [0211], and performing mutual authentication with the first apparatus so as to establish a first

encrypted communication channel (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209];

a part for exchanging key information for encrypted communication with the second apparatus, and performing mutual authentication with the second apparatus so as to establish a second encrypted communication channel (i.e. The exchange of session key information) [0214];

a part for receiving a public-key of the first apparatus via the first encrypted communication channel [0219-0222];

a part for storing the received public-key in its storage device [0219-0222]; and

a part for sending the public-key of the first apparatus via the second encrypted communication channel to the second apparatus [0219-0222].

As to claim 31, Birger discloses that the public-key management apparatus includes a first apparatus for establishing the first encrypted communication channel and the second encrypted communication channel, and a second apparatus that is connected to the first apparatus and that manages public-keys [0219-0222].

As to claim 32, Birger discloses the public-key management apparatus as claimed in claim 30, the public-key management apparatus further comprising:

a part for performing message communications between the first apparatus and the public-key management apparatus and between the second apparatus and the public-key management apparatus by using Session Initiation Protocol [0219-0222].

As to claim 34, Birger discloses a computer program for causing a computer to function as a public-key management apparatus for managing public-keys used for establishing an encrypted communication channel between a first apparatus and a second apparatus, the computer program comprising:

program code means for exchanging key information used for encrypted communication with the first apparatus (i.e. The exchange of session key information.) [0211], and performing mutual authentication with the first apparatus so as to establish a first encrypted communication channel (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209];

program code means for exchanging key information for encrypted communication with the second apparatus, and performing mutual authentication with the second apparatus so as to establish a second encrypted communication channel (i.e. The exchange of session key information) [0214];

program code means for receiving a public-key of the first apparatus via the first encrypted communication channel [0219-0222];

program code means for storing the received public-key in a storage device [0219-0222]; and

program code means for sending the public-key of the first apparatus via the second encrypted communication channel to the second apparatus [0219-0222].

As to claim 35, Birger discloses a session management apparatus that can connect to a first apparatus and a second apparatus over a network, the session management apparatus comprising:

a part for performing mutual authentication with the first apparatus to establish a first encrypted communication channel between the session management apparatus and the first apparatus (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209], and storing a name of the first apparatus and identification information of the first encrypted communication channel in a storage device wherein the name of the first apparatus and the identification information are associated with each other (i.e. unique identifier) [0174];

a part for establishing a second encrypted communication channel between the session management apparatus and the second apparatus based on mutual authentication with the second apparatus (i.e. the second phase is session management that includes conducting mutual authentication) [0216];

a part for receiving a message including a name of the first apparatus via the first encrypted communication channel (i.e. unique identifier) [0174];

a part for determining whether the name included in the message is correct by comparing the name included in the message with the name that is stored in the storage device and that is associated with the identification information of the first encrypted communication channel [0250]; and

a part for sending the message to the second apparatus via the second encrypted communication channel [0257].

As to claim 36, Birger discloses that if the session management apparatus determines that the name of the first apparatus included in the message is not correct, the session management apparatus sends an error message to the first apparatus [0051].

As to claim 37, Birger discloses a session management apparatus that can connect to a first apparatus and a second apparatus over a network, the session management apparatus comprising:

a part for performing mutual authentication with the first apparatus to establish a first encrypted communication channel between the session management apparatus and the first apparatus (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209];

a part for establishing a second encrypted communication channel between the session management apparatus and the second apparatus based on mutual authentication with the second apparatus (i.e. the second phase is session management that includes conducting mutual authentication) [0216];

a part for receiving, from the first apparatus via the first encrypted communication channel, a message including a first header indicating reliability of a route between the first apparatus and the session management apparatus (i.e. quality of service) [0275]; and

a part for adding a second header indicating reliability of a route between the session management apparatus and the second apparatus to the message, and sending the message to the second apparatus via the second encrypted communication channel (i.e. quality of service) [0275].

As to claim 38, Birger discloses that the first header includes an address of the first apparatus, and in response to receiving the first header, the session management apparatus determines validity of the first header by comparing an address included in the first header and an address of the first apparatus (i.e. authenticating addresses) [0090].

As to claim 39, Birger discloses that the message is based on Session Initiation Protocol [0241].

As to claim 40, Birger discloses a method for transferring a message among a first apparatus, a session management apparatus and a second apparatus each connected to a network, wherein:

the session management apparatus and the first apparatus perform mutual authentication to establish a first encrypted communication channel between the session management apparatus and the first apparatus (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209], and the session management apparatus stores a name of the first apparatus and identification information of the first encrypted communication channel in a storage device wherein the name of the first apparatus and the identification information are associated with each other (i.e. unique identifier) [0174];

the session management apparatus and the second apparatus performs mutual communication to establish a second encrypted communication channel between the session management apparatus and the second apparatus (i.e. the second phase is session management that includes conducting mutual authentication) [0216];

the first apparatus sends a message including a name of the first apparatus via the first encrypted communication channel to the session management apparatus (i.e. the unique identifier) [0174];

the session management apparatus determines whether the name included in the message is correct by comparing the name included in the message with the name that is stored in the storage device and that is associated with the identification information of the first encrypted communication channel [0250]; and

the session management apparatus sends the message to the second apparatus via the second encrypted communication channel [0257].

As to claim 41, Birger discloses a method for transferring a message among a first apparatus, a session management apparatus and a second apparatus each connected to a network, wherein:

the session management apparatus and the first apparatus perform mutual authentication to establish a first encrypted communication channel between the session management apparatus and the first apparatus (i.e. The registration

process involves a mutual authentication between the endpoint and the authentication service.) [0209];

the session management apparatus and the second apparatus perform mutual communication to establish a second encrypted communication channel between the session management apparatus and the second apparatus (i.e. the second phase is session management that includes conducting mutual authentication) [0216];

the first apparatus sends, to the session management apparatus via the first encrypted communication channel, a message including a first header indicating reliability of a route between the first apparatus and the session management apparatus (i.e. quality of service) [0275]; and

the session management apparatus adds a second header indicating reliability of a route between the session management apparatus and the second apparatus to the message, and sends the message to the second apparatus via the second encrypted communication channel (i.e. quality of service) [0275].

As to claim 42, Birger discloses a computer program for causing a computer to function as a session management apparatus that can connect to a first apparatus and a second apparatus over a network, the computer program comprising:

program code means for performing mutual authentication with the first apparatus to establish a first encrypted communication channel between the session management apparatus and the first apparatus (i.e. The registration process involves a mutual authentication between the endpoint and the

authentication service.) [0209], and storing a name of the first apparatus and identification information of the first encrypted communication channel in a storage device wherein the name of the first apparatus and the identification information are associated with each other (i.e. unique identifier) [0174];

program code means for establishing a second encrypted communication channel between the session management apparatus and the second apparatus based on mutual authentication with the second apparatus (i.e. the second phase is session management that includes conducting mutual authentication) [0216];

program code means for receiving a message including a name of the first apparatus via the first encrypted communication channel (i.e. unique identifier) [0174];

program code means for determining whether the name included in the message is correct by comparing the name included in the message with the name that is stored in the storage device and that is associated with the identification information of the first encrypted communication channel [0250]; and

program code means for sending the message to the second apparatus via the second encrypted communication channel [0257].

As to claim 43, Birger discloses a computer program for causing a computer to function as a session management apparatus that can connect to a first apparatus and a second apparatus over a network, the computer program comprising:

program code means for performing mutual authentication with the first apparatus to establish a first encrypted communication channel between the

session management apparatus and the first apparatus (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209];

program code means for establishing a second encrypted communication channel between the session management apparatus and the second apparatus based on mutual authentication with the second apparatus (i.e. the second phase is session management that includes conducting mutual authentication) [0216];

program code means for receiving, from the first apparatus via the first encrypted communication channel, a message including a first header indicating reliability of a route between the first apparatus and the session management apparatus (i.e. quality of service) [0275]; and

program code means for adding a second header indicating reliability of a route between the session management apparatus and the second apparatus to the message, and sending the message to the second apparatus via the second encrypted communication channel (i.e. quality of service) [0275].

Conclusion

9. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ARAVIND K. MOORTHY whose telephone number is (571)272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Thomas can be reached on 571-272-6776. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/
Primary Examiner, Art Unit 2492